5 FAH-11 H-000 INFORMATION ASSURANCE HANDBOOK

5 FAH-11 H-010 INTRODUCTION

(CT:IAH-1; 02-15-2007)
(Office of Origin: IRM/IA)

5 FAH-11 H-011 PURPOSE

(CT:IAH-1; 02-15-2007)

a. The Bureau of Information Resource Management, Office of Information Assurance (IRM/IA), establishes procedures to manage the security of the Department's information and information systems efficiently and effectively.

b. This handbook supplements the policy established in 5 FAM 1060, Information Assurance Management. It complies with the Federal Information Security Management Act of 2002 (FISMA) requirements for the Chief Information Officer (CIO) and agency program officials, and establishes cyber-security roles and responsibilities to manage the security of the Department's information and information systems.

c. Direct questions and suggestions regarding security of the Department's information and information systems found in this handbook to IRM/IA.

5 FAH-11 H-012 SCOPE AND APPLICABILITY

(CT:IAH-1; 02-15-2007)

a. These procedures apply to all Department entities with information systems.

b. This handbook also includes procedures for other entities (e.g., contractors, other agencies, and organizations) that exchange or process Department information on their systems through interconnections with the Department, or alternatively, are linked to the Department via extensions of the Department networks.

c. The procedures in this handbook are not applicable to sensitive compartmented information (SCI) systems.

5 FAH-11 H-013 HANDBOOK CONTENTS

(CT:IAH-1; 02-15-2007)

a. This handbook is composed of nine chapters that cover the following:

(1) 5 FAH-11 **H-000** elaborates on the policy requirements established in 5 FAM 1060 and supports the CIO's and agency program officials' requirements under FISMA. It also establishes cyber-security roles and responsibilities to manage the security of the Department's information and information systems;

(2) **5 FAH-11 H-100** provides duties and implementing procedures for the Department's Information Systems Security Officer (ISSO) Program;

(3) **5 FAH-11 H-200** demonstrates how to perform an information security audit to accomplish a system's certification;

(4) **5 FAH-11 H-300** provides a comprehensive approach to the Department's Systems Authorization Process;

(5) **5 FAH-11 H-400** establishes a comprehensive approach to non-Department systems authorization;

(6) **5 FAH-11 H-500** provides implementing procedures for establishing performance measures for Information Assurance. It explains how system owners and managers must work together to ensure that performance metrics are applied for Department information technology (IT) personnel who are assisting in developing, implementing, and managing an IT security program (see 5 FAM 130);

(7) **5 FAH-11 H-600** provides a convenient point of reference for the minimum mandatory information system security controls required for cyber systems, sites, and types, and maps the

controls to established Federal requirements and Department policies and regulations;

(8) **5 FAH-11 H-700** provides the procedures for evaluating location-specific systems cyber security controls at facilities that process or store Department information on automated information systems (AISs) for FISMA compliance; and

(9) **5 FAH-11 H-800** provides procedures for planning, establishing, maintaining, and terminating interconnections between information technology systems of non-Department entities and the Department of State, as well as guidance for extensions of the Department's OpenNet and ClassNet networks.

b. All Department personnel must comply with the requirements in the chapters listed in paragraph a of this section.

5 FAH-11 H-014 DEFINITIONS AND TERMS USED IN THIS HANDBOOK AND IN 5 FAM 1060

(CT:IAH-1; 02-15-2007)

These are the definitions and terms that relate to information assurance as found in the 5 FAM 1060 and this Handbook.

Accreditation: The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation) or agency assets, based on the implementation of an agreed upon set of security controls.

Certification: (See 5 FAM 814.)

Chief Information Officer (CIO): (See 5 FAM 820.)

Chief Information Security Officer (CISO): (See 5 FAM 820.)

Confidentiality: The assurance that information in an IT system is not disclosed to unauthorized persons, processes, or devices.

Configuration Management: (See 5 FAM 613.)

Contingency Planning: Security controls dealing with emergency response, backup operations, and post-disaster recovery for an IT system to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Defense in Depth: A practical strategy for achieving Information Assurance by applying security measures to all components of the system, creating a security architecture that calls for the network to be aware and self-protective. It is a "best practices" strategy that relies on the intelligent application of techniques and technologies. The strategy recommends a balance between the protection capability and cost, performance, and operational considerations.

Designated Approving Authority (DAA): (See 5 FAM 814.)

Evaluation Assurance Level (EAL): An assurance requirement as defined by Common Criteria, an international standard in effect since 1999, to replace the ratings (e.g., "C2") found in the Orange Book that were set by the National Computer Security Center (NCSC). The increasing assurance levels (i.e., EAL1 through EAL7) define increasing assurance requirements in computer systems. These levels are:

- EAL1: Functionally Tested
- EAL2: Structurally Tested
- EAL3: Methodically Tested and Checked
- EAL4: Methodically Designed, Tested and Reviewed
- EAL5: Semiformally Designed and Tested
- EAL6: Semiformally Verified Design and Tested
- EAL7: Formally Verified Design and Tested

Enterprise Architecture: (See 5 FAM 674.)

Federal Information System: An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. (See 40 U.S.C. 11331.)

General Support System: An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Information Security: Operations to protect and defend information and IT systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IT systems by incorporating protection, detection, and reaction capabilities.

Information System: The set of agency information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Categories of IT systems are major applications and general support systems.

Information System Security Officer (ISSO): (See 5 FAM 820.)

Information Technology: (See 5 FAM 913.)

Information Type: A specific category of information (e.g., medical, proprietary, financial, investigative, contractor-sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Integrity Assurance: Information in an IT system is protected from unauthorized, unanticipated or unintentional modification or destruction. Integrity assurance also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data.

Major Application: An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might compromise many individual application programs and hardware, software and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Management Controls: The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk for the system. Management controls include risk management, review of security controls, system lifecycle controls, processing authorization controls, system security plan controls, and privacy controls.

Minor Application: An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

Operational Controls: The controls that address security mechanisms implemented and executed primarily by people (as opposed to systems).

Penetration Testing: Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify methods of gaining access to a system by using common tools and techniques used by attackers.

Plan of Action and Milestones (POA&M): A management tool for identifying corrective action that needs to be taken to mitigate vulnerability. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Potential Impact Level: Federal Information Processing Standards (FIPS) Publication 199 defines three levels of potential impact—low, moderate, and high—on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

Remediation: The act or process of remedying system or information assurance deficiencies, vulnerabilities, or weaknesses discovered and documented in due course of operational checks, controls, evaluations, or audits.

Risk: The net mission impact considering: (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular IT system vulnerability; and (2) the resulting impact if this should occur. IT system-related risks arise from legal liability or mission loss due to:

(1) Unauthorized (malicious or accidental) disclosure, modification, or destruction of information;

(2) Unintentional errors and omissions;

(3) IT disruptions due to natural or man-made disasters; and

(4) Failure to exercise due care and diligence in the implementation and operation of the IT system.

Risk Assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. This is part of risk management and synonymous with risk analysis.

Risk management: (See 5 FAM 613.)

Security Categories: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

5 FAH-11 H-015 THROUGH H-019 UNASSIGNED